

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

United States of America

v.

REYNALDO MOGUEL-BONILLA,
MARIA DEL CARMEN ANDRADE,
OSCAR GUEVARA, and
OMAR GUEVARA

Case No.

14-M-1287

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 2013 to present in the county of Milwaukee in the
Eastern District of Wisconsin, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 1028

Fraud and related activity in connection with identification documents, authentication features, and information

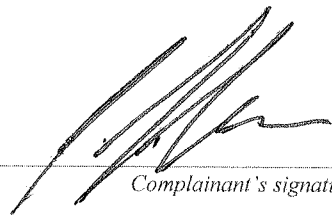
18 U.S.C. § 1546

Fraud and misuse of visas, permits, and other documents

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.



Complainant's signature

Special Agent Ian House, DHS HSI ICE

Printed name and title

Sworn to before me and signed in my presence.

Date:

11/18/14

City and state: Milwaukee, Wisconsin



Judge's signature

William E. Duffin, US Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT,
CRIMINAL COMPLAINT, AND ARREST WARRANTS**

I, Ian House, Special Agent, United States Department of Homeland Security, Homeland Security Investigations, being duly sworn and under oath state the following:

EXPERIENCE OF AFFIANT

1. I am a Special Agent with United States Homeland Security Investigations (HSI) under Immigration and Customs Enforcement (ICE), comprised of the former United States Immigration and Naturalization Service (INS) and United States Customs Service. I have been employed by HSI since August 2008. I am currently assigned to the HSI Resident Agent in Charge (RAC), Office of Investigations, in Milwaukee, Wisconsin.
2. Prior to my current assignment, I was a United State Customs and Border Protection (CBP) Officer at the Pembina, ND Port of Entry. I was employed by CBP for more than three years, from May 2005 to August 2008. While working as a CBP Officer, I was tasked with training new officers regarding the proper procedures relating to identifying and enforcing the Immigration and Customs laws of the United States, as well as any federal laws at the international border.
3. I have received training in fraudulent document detection from ICE/HSI. In February 2010, I was certified as a fraudulent document detection trainer.
4. In my current employment, I am assigned to investigate alleged violations of the Immigration and Nationality Act (INA). This includes the enforcement of laws prohibiting the unlawful production, possession, use or distribution of counterfeit immigration and identity documents.

PURPOSE OF AFFIDAVIT

5. This affidavit is made in support of the following:
- (a) an application under Federal Rule of Criminal Procedure 41 for a warrant to search the premises known as 1610 South 35th Street, Milwaukee, Wisconsin, described further in Attachment A (the “**Subject Premises**”), for the things described in Attachment B; and
 - (b) a criminal complaint and arrest warrants for the following individuals:
 - i. **Reynaldo Moguel-Bonilla**;
 - ii. **Maria Del Carmen Andrade** (also referred to as **Maria Del Carmen Andrade-Cendejas**);
 - iii. **Oscar Guevara**;
 - iv. **Omar Guevara** (also referred to as **Omar Guevara-Barajas**)
6. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, complaints and arrest warrants, I have not included each and every fact known to me concerning this investigation. I have only set forth those facts that I believe are essential to establish sufficient probable cause that **Oscar Guevara**, **Omar Guevara-Barajas**, **Maria Del Carmen Andrade-Cendejas**, and **Reynaldo Moguel-Bonilla**, committed violations of Title 18, United States Code, Sections 1028(a) and 1546; and that evidence, instrumentalities, fruits, and contraband concerning violations

of Title 18, United States Code, Sections 1028 and 1546 are located at the **Subject Premises.**

(a) **Omar Guevara** was ordered deported from the United States by an immigration judge in November, 2013. He is currently appealing the order.

(b) **Oscar Guevara, Maria Del Carmen Andrade, and Reynaldo Moguel-Bonilla** all appear to be present in the US without authorization. No records of legal crossings into the US or any pending or approved immigration applications or petitions were discovered relating to the participants. Any Social Security numbers used by the participants for utility services appear to be either fabricated or previously issued to someone else.

BACKGROUND INFORMATION

7. The United States Office of Citizenship and Immigration Services ("CIS") is a division or section of the United State Department of Homeland Security. The United States government through CIS is the only entity authorized to issue a United States I-551 Permanent Resident Card ("I-551 card"). An I-551 card is issued to a foreign national who has been granted permanent legal status to reside in the United States and obtain employment in the United States.
8. The United States government through the Social Security Administration is the only entity authorized to issue United States social security cards and account numbers.

9. Through my training, experience, and discussions with other experienced agents, I know the following:

- (a) Individuals involved in the sale, transfer and production of fraudulent documents often use numerous electronic devices to communicate with customers and to manufacture documents. Fraudulent document vendors commonly use cell phones that do not require subscriber information or billing information to conduct their illegal enterprises. The phones enable vendors to communicate with their clients with a lesser risk of detection. These cell phones are easily disposed of in the event the user believes the authorities have discovered its use.
- (b) One of the most common methods of manufacturing fraudulent documents is through use of computers and printers. Computers and photographic equipment enable fraudulent document vendors to create various types of documents using a single image of their customer.
- (c) Fraudulent document vendors often times advertise their products through word of mouth and business cards. Often the business cards have an innocuous business identified as the primary purpose, product or service such as "dog grooming," "bike repair," "photography," or "auto body repair" when in fact the business cards are used for the purpose of providing the vendor's contact information to a customer interested in obtaining fraudulent documents.
- (d) Individuals who manufacture counterfeit identification documents often use countermeasures to frustrate law enforcement officers, including

meeting customers at locations unassociated with the production of fraudulent documents.

STATUTES

10. This investigation concerns alleged criminal violations of Title 18, United States Code, Sections 1028, and 1546.
11. Title 18, United States Code, Section 1028(a)(1) makes it unlawful to knowingly and without lawful authority produce an identification document, authentication feature or a false identification document.
12. Title 18, United States Code, Section 1028(a)(2) makes it unlawful to knowingly transfer a false identification document, knowing that such document was produced without lawful authority.
13. Title 18, United States Code, Section 1028(a)(3) makes it unlawful to knowingly possess with intent to use unlawfully or transfer unlawfully 5 or more identification documents (other than those issued lawfully for the use of the processor).
14. Title 18, United States Code, Section 1028(a)(5) makes it unlawful to knowingly produce, transfer, or possess a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature.
15. Title 18, United States Code, Section 1028(d)(1) defines an authentication feature as “any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with

- another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered or otherwise falsified.”
16. Title 18, United States Code, Section 1028(d)(3), in pertinent part, defines an identification document as “a document made or issued by or under the authority of the United States Government...which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals.”
17. Title 18, United States Code, Section 1028(d)(4) defines a false identification document as “a document of a type intended or commonly accepted for the purposes of identification of individuals that: (A) is not issued by or under the authority of a government entity...; and (B) appears to be issued by or under the authority of the United States Government....”
18. Title 18, United States Code, Section 1546(a) makes it unlawful to knowingly counterfeit or falsely make an alien registration receipt card or other document prescribed by statute or regulation for entry into or as evidence of authorized stay or employment in the United States.

CONTROLLED PURCHASES OF COUNTERFEIT DOCUMENTS

19. In June 2013, I received from unrelated sources three business cards advertising house painters. I was informed that each one was actually used to advertise the creation and purchase of counterfeit documents. Each card had a different name and phone number: “Luis”: 414-215-6304; “Sammy”: 414-215-4560; and “Xavier”: 414-698-9481.

- (a) On July 1, 2013, a confidential informant (CI-1),¹ under the direction of HSI Milwaukee, dialed each phone number. For each call, CI spoke to a different Spanish speaking male and confirmed that each one would sell to CI-1 counterfeit documents. Each of the males stated that the cost for the “package” of documents, including a counterfeit I-551 resident alien card and Social Security card, was approximately \$170.00 USD.
- (b) Subpoenas for these numbers revealed that (1) 414-215-6304 was listed to an account of “Luis Lopez” with no address provided; (2) 414-215-4560 had no records associated with it; (3) 414-698-9481 was listed to an account of **Maria Del Carmen Andrade**.

Controlled Transaction of March 10, 2014 involving Reynaldo Moguel-Bonilla

20. On March 10, 2014, the CI-1, under the control of HSI Milwaukee, dialed the cellular telephone number 414-215-3607. HSI has received this number from a concerned citizen, and CI-1 had previously dialed the number in order to determine its authenticity for selling counterfeit documents. CI-1 spoke to a male identifying himself as “Luis” in the Spanish language and scheduled to meet to place an order for a counterfeit I-551 resident alien card and a counterfeit Social Security card. The meeting was to take place at the corner of West Lincoln Avenue and South 17th Street, Milwaukee, Wisconsin, around 1400hrs that day.

“Luis” informed CI-1 that he was driving a white 4-door pick-up truck.

¹ CI-1 has been cooperating with law enforcement since 2005 and in this investigation since 2013. CI-1 has two prior convictions. CI-1 is primarily cooperating with law in exchange for an immigration status. To date, CI-1 has continuously received immigration benefits in exchange for his/her cooperation and has had no other arrests or convictions. CI-1 has repeatedly provided law enforcement with reliable and timely information in this investigation that has been corroborated by recorded phone calls, covert meetings, and other law enforcement reporting.

21. Surveillance agents at the proposed meeting location observed a white Chevrolet Colorado pick-up truck with WI License Plate #JQ5902 arrive at 1402hrs. CI-1 then arrived at the location in his/her vehicle. Agents then observed a Hispanic male exit the Colorado and approach CI-1's vehicle. The Hispanic male identified himself to CI-1 as "Luis." Luis then directed CI-1 to a nearby stairwell and took a photograph of CI-1. CI-1 also told Luis what information he wanted on the counterfeit I-551 card. A few minutes later, Luis and CI-1 departed the area in their vehicles. Agents followed Luis's vehicle, which made several stops at various locations.

22. Shortly before 1500hrs, "Luis" called CI-1 and said that the documents were ready and that they should meet at the same location as the previous meeting. At approx. 1507hrs, "Luis" met CI-1. CI-1 handed \$170.00 in pre-recorded currency to "Luis", who in turn handed the counterfeit documents to CI-1. They then left the scene.

(a) Examination of the documents provided by "Luis" to CI-1 revealed that they lacked security features of genuine documents. The counterfeit I-551 card showed CI-1 with a fictitious name and date of birth. The alien registration number on the I-551 card was one that had been previously issued by CIS to a person later removed from the United States. The counterfeit Social Security Card showed a number that was previously issued to someone in California.

23. Following the transaction, agents checked the history of the White Chevrolet Colorado bearing license plate WI#JQ5902. That vehicle was registered to a

Catalina Arellano-Castro, residing at 2633 West Beecher St., Milwaukee, WI. Agents observed "Luis" go to this address during surveillance. According to HSI databases, Arellano-Castro resides with **Reynaldo Moguel-Bonilla**. Further, records from WE Energies for 2633 West Beecher St., Milwaukee, WI show that **Reynaldo Moguel-Bonilla** is utility account holder for that address.

24. I reviewed a driver's license photograph of **Reynaldo Moguel-Bonilla** and believe that he is "Luis," whom I observed while doing surveillance of the transaction on March 10, 2014. CI-1 also reviewed the driver's license photograph of **Reynaldo Moguel-Bonilla** and confirmed that the person in the photograph is "Luis" from the March 10, 2014 transaction.

Controlled Transaction of August 18, 2014 involving Oscar Guevara

25. On August 18, 2014, CI-1, under the control of HSI Milwaukee, dialed the cellular telephone number, 414-698-9481, and spoke to "Xavier" in order to purchase counterfeit documents. The CI-1 spoke to a Spanish-speaking male, and agreed to meet at El Rey grocery store, located at the corner of South 13th St. and West Mitchell St., Milwaukee, WI at 1130hrs. CI-1 was told to call upon arriving.
26. Upon arriving, CI-1 called "Xavier." "Xavier" told CI-1 that he was driving a minivan. A few minutes later, a Kia Sedona with Wisconsin license plate #435UVW arrived and the driver motioned to CI-1 to approach the vehicle. The driver told CI-1 to enter the vehicle and sit in the front seat. CI-1 and the driver spoke for a few minutes, and then CI-1 exited the Kia Sedona and Sedona drove away.

27. Surveillance agents queried the registration of the Sedona. The license plate and vehicle were registered to **Oscar Guevara**, residing at 3406 St. Paul Ave., Milwaukee, WI. His date of birth was listed as March 6, 1977.
28. Surveillance agents followed the Sedona. It eventually stopped near the corner of South 18th St. and West Lincoln Ave. in Milwaukee.
29. CI-1 later received a call from "Xavier" stating that they should meet the intersection of West Lincoln Ave. and South 17th St. CI-1 met "Xavier" at that location a few minutes later and "Xavier" handed CI-1 a counterfeit I-551 resident alien card and a counterfeit Social Security card in exchange for \$170.00 in pre-recorded currency. "Xavier" also handed CI-1 some business cards with his phone number on it to hand out to other potential customers. "Xavier" then departed.
- (a) Examination of the documents provided by "Xavier" to CI-1 revealed that they lacked security features of genuine documents. The counterfeit I-551 card showed CI-1 with a fictitious name and date of birth. The alien registration number on the I-551 card was one that had been previously issued by CIS to a naturalized U.S. citizen from Korea. The counterfeit Social Security Card listed a number that had not been previously issued by the Social Security Administration.
30. On August 20, 2014, I met with CI-1 and showed CI-1 a photograph of **Oscar Guevara**, who was the registered owner of the Kia Sedona used in the August 18, 2014 controlled transaction. CI-1 confirmed that **Oscar Guevara** is "Xavier" from the August 18, 2014 transaction.

August 25, 2014 Controlled Transaction involving Oscar Guevara
and Omar Guevara

31. On August 25, 2014, CI-1, under the control of HSI Milwaukee, dialed the cell phone number 414-304-4464 and spoke to a Spanish-speaking male in order to try to purchase counterfeit documents. This phone number was listed on a business card for "Fotographia" with the name "Jorge," and was handed to CI-1 by **Oscar Guevara** during the August 18, 2014 controlled transaction.
32. During the phone call, CI-1 and the male, whom CI-1 stated s/he believed to be the same person from the August 18, 2014 transaction, agreed to meet at the El Rey grocery store at the intersection of West Burnham St. and South 13th St. in Milwaukee, WI. HSI Milwaukee agents provided CI with a photograph of a Hispanic male that CI-1 would give to the counterfeit maker to produce the counterfeit documents.
33. CI-1 arrived at the agreed upon location. A few minutes later, a green Honda Accord with Wisconsin license plate #815WDL arrived. The vehicle was driven by a Hispanic male. The Hispanic male driver and CI-1 spoke for a few minutes, and then the Hispanic male drove away. A query of the Honda Accord's registration indicated that the vehicle is registered to a **Maria Del Carmen Andrade-Cendejas**, residing at 3406 West St. Paul Ave., Milwaukee, WI, which was the same address as **Oscar Guevara**.
34. Believing that the vehicle may travel to the area of South 18th Street and West Lincoln Avenue, where the transactions of March 10, 2014 and August 18, 2014 occurred, I proceeded to that location after the initial meeting between CI-1 and the Hispanic male at the El Ray grocery store. A few minutes later, the green

Honda Accord with #815WDL arrived at the intersection of West Lincoln Ave. and South 18th St. The vehicle parked a few yards in front of me and I observed the driver to be **Oscar Guevara**. Agents observed **Oscar Guevara** enter a door on the east side of 1720 West Lincoln Avenue.

35. While waiting for **Oscar Guevara** to reappear, agents observed **Omar Guevara** arrive at the location in a silver Hyundai with Wisconsin license plate #609VDF. **Omar Guevara** and an unknown female exited the vehicle and went the same way that **Oscar Guevara** had gone.

36. A short time later, agents observed **Omar Guevara** outside on the rear porch of second level at 1720 West Lincoln Ave. He dropped a cell phone to the unknown female he arrived with and she departed in silver Hyundai with Wisconsin license plate # 609VDF.

37. CI-1 then received a call from **Oscar Guevara** stating that the documents were ready and that that they should meet at the El Rey parking lot.

38. At the El Rey parking lot, **Oscar Guevara** provided CI-1 with a counterfeit I-551 resident alien card and counterfeit Social Security card in exchange for \$170.00 in pre-recorded currency.

(a) Examination of the documents provided to CI-1 revealed that they lacked security features of genuine documents. The counterfeit I-551 card showed CI-1 with a fictitious name and date of birth. The alien registration number on the I-551 card was one that had not been previously issued by CIS. The counterfeit Social Security Card listed a number previously

issued by the Social Security Administration to a person in South Dakota prior to 1951.

39. After the transaction, agents followed **Oscar Guevara**, who proceeded to 3406 West St. Paul Ave, Milwaukee, WI.

40. Following the transaction, agents queried the address of 1720 West Lincoln Ave, Milwaukee. The results showed that the building has four separate units. **Omar Guevara-Barajas** was listed as the tenant of the upper rear unit.

Controlled Transaction of September 24, 2014 involving Omar Guevara and Maria Del Carmen Andrade

41. On September 23, 2014, a law enforcement agent with the State of Wisconsin acting in an undercover capacity ("UC-1"), and working with HSI Milwaukee, placed a recorded phone call to phone number 414-304-4464 to attempt to purchase counterfeit documents. This is the same number used for the August 25, 2014 controlled transaction. UC-1 spoke to a Hispanic male, who said he could get the documents requested.

42. UC-1 was directed to meet the Hispanic male in the parking lot at Chicken Palace, 3433 W. National Ave., Milwaukee, WI. The male said he was driving a silver sedan. At that location, UC-1 met the male, who was in silver Hyundai Elantra with Wisconsin license plate #627WJS.

(a) This vehicle was previously identified as being registered to **Omar Guevara-Barajas**.

43. UC-1 entered the Hyundai and provided the male with a document containing five photographs and fictitious names and date of birth to be used to make five sets of

counterfeit documents. They agreed on a total price of \$850.00. UC-1 then exited the vehicle.

(a) Upon review of a known photograph of **Omar Guevara**, UC-1 identified **Omar Guevara** as the person he met with.

44. Surveillance followed **Omar Guevara**, who drove to the 1600 block of South 35th Street, Milwaukee, WI.

45. UC-1 and **Omar Guevara** had several conversations during the day about when the documents would be ready. During one of the conversations, **Omar Guevara** indicated that the documents were being prepared by a female. They agreed to meet the following day.

46. The next day, September 24, 2014, agents began surveillance around the 1600 block of South 35th Street, where **Omar Guevara** was observed the previous evening. **Omar Guevara's** vehicle was located by agents on a parking slab behind 1610 South 35th Street ("**Subject Premises**").

47. In conversations that morning, UC-1 and **Omar Guevara** agreed to meet at the El Rey grocery store, 3524 W. Burnham St. Milwaukee, WI. Surveillance agents observed **Omar Guevara** and a female depart the **Subject Premises** and proceed to the El Rey grocery store. **Omar Guevara** parked the vehicle near the store and waived UC-1 over to his vehicle.

48. UC-1 entered the rear passenger side of **Omar Guevara's** vehicle. The female, later confirmed by UC-1 as **Maria Del Carmen Andrade**, was in the front passenger seat. UC-1 provided **Omar Guevara** with \$850 in prerecorded

currency and **Omar Guevara** provided UC-1 with five counterfeit I-551 cards and five counterfeit Social Security cards.

- (a) Examination of the documents provided UC-1 revealed that they lacked security features of genuine documents. The counterfeit I-551 cards showed fictitious names and date of births. The alien registration numbers on the I-551 cards were reviewed; four of the cards had numbers that had previously been issued by CIS and one had a number that had not been previously issued by CIS. The counterfeit Social Security cards showed the fabricated information supplied by UC-1.

49. **Omar Guevara** also handed UC-1 two new business cards with new names and phone numbers.

- (a) One card lists the name “Diego” with phone number 414-839-1340. A query of HSI databases shows this number is has been previously used by **Omar Guevara** to open utility services.

- (b) One card lists the name “Angel” with phone number 414-400-8600.

50. To determine if **Omar Guevara** moved residences, agents subpoenaed records from WE Energies for the residence at 1610 South 35th Street, Milwaukee, WI, (**Subject Premises**) and the residence 1720 West Lincoln Ave, Milwaukee, WI, where a previous record check listed **Omar Guevara** as the account holder. Records obtained from WE Energies on October 20, 2014, show that **Omar Guevara** terminated utility service at 1720 West Lincoln Ave. and then opened a new account for 1610 South 35th Street (**Subject Premises**).

(a) In addition, the WE Energies records listed **Omar Guevara's** cell phone number as 414-839-1340, which is the same number on one of the business cards handed by **Omar Guevara** to UC-1 during the September 24, 2014 controlled transaction.

Transaction of October 28, 2014 involving Omar Guevara
and Maria Del Carmen Andrade.

51. On October 28, 2014, the UC-1, working with HSI Milwaukee, placed a call to phone number 414-400-8600, which was printed on one of the business cards handed to UC-1 by **Omar Guevara** during the September 24, 2014 controlled transaction, to try to purchase counterfeit documents. **Omar Guevara** answered the phone and they agreed to meet at the Chicken Palace, at South 35th Street and National Avenue in Milwaukee, WI, at 1100hrs.

52. After the call, agents went to conduct surveillance at the **Subject Premises**. Omar Guevara's silver Hyundai with Wisconsin license plate #627WJS, the vehicle used in the September 24, 2014 controlled transaction, was parked at the residence. While waiting for **Omar Guevara** to depart, agents observed a **Reynaldo Moguel-Bonilla** arrive at the Subject Premises in a green pick-up truck with Wisconsin license plate #FN1014, which is registered to **Reynaldo Moguel-Bonilla**. **Reynaldo Moguel-Bonilla** exited the truck and walked in the direction of Omar Guevara's residence. He returned a minute later and departed. Based on my training, experience, and the observations of **Reynaldo Moguel-Bonilla** during the March 10, 2014 controlled transaction, it appeared he may have delivered an order for counterfeit documents to be created.

53. Around 1100hrs, UC-1 called **Omar Guevara** and surveillance agents then observed **Omar Guevara** depart the **Subject Premises** in the silver Hyundai.
54. Around 1110hrs, **Omar Guevara** arrived at the Chicken Palace and spoke to UC-1. UC-1 placed an order for a counterfeit I-551 card and counterfeit Social Security card. **Omar Guevara** told UC-1 that the order would take around 40 minutes to complete and they arranged to meet at the El Rey grocery store at 35th Street and West Burnham Avenue, Milwaukee, WI.
55. Surveillance agents followed **Omar Guevara** after the meeting. **Omar Guevara** was observed entering and exiting stores for grocery purchases and appeared to hand out business cards at an El Rey grocery store. Around 1148hrs, **Omar Guevara** arrived at the **Subject Premises**. A few minutes after he arrived, agents observed **Oscar Guevara** arrive and carry a bag into the **Subject Premises**.
56. At around 1215hrs, UC-1 called **Omar Guevara** and asked if the documents were ready. **Omar Guevara** responded that they would be ready in 10 minutes.
57. Around 1236hrs, agents observed **Omar Guevara** and a female leave the **Subject Premises** in the silver Hyundai and proceed to the El Rey grocery store. At the El Rey store, UC-1 walked over and got in **Omar Guevara's** vehicle. At that time, **Omar Guevara** provided UC-1 with a counterfeit I-551 card and counterfeit Social Security card in exchange for \$170 in prerecorded currency.
- (a) Examination of the documents provided to UC-1 revealed that they lacked security features of genuine documents. The counterfeit I-551 card showed CI-1 with a fictitious name and date of birth. The alien registration number on the I-551 card was one that had been previously issued by CIS

to a person later removed from the United States. The counterfeit Social Security Card listed the fabricated information supplied by UC-1.

58. UC-1 confirmed that the female inside **Omar Guevara's** vehicle was **Maria Del Carmen Andrade**, who was the same female with **Omar Guevara** during the September 23, 2014 controlled transaction.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

59. As described above and in Attachment B, this application seeks permission to search for documents and records that might be found on the Subject Premises, in whatever form they are found. One form in which the documents and records might be found is data stored on a computer's hard drive or other storage media. Storage media is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

60. *Probable cause.* I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- (a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted,

they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

(b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

(c) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

(d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

61. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that

establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

- (a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- (b) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the

foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- (c) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- (d) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- (e) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

62. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- (a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- (b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application

software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

(c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

63. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

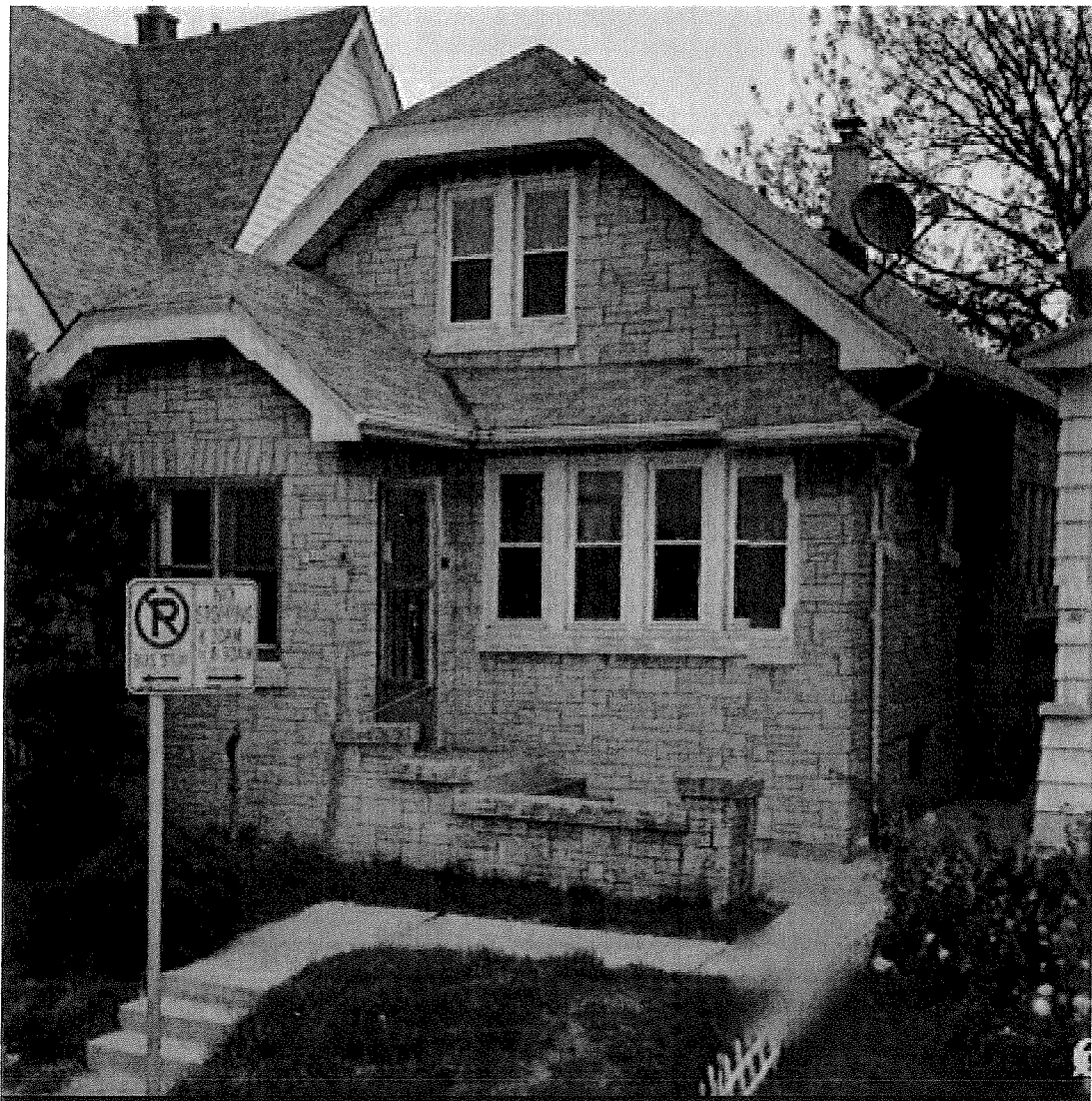
64. Based on the above information, I believe probable cause exists to search the **Subject Premises** located at 1610 South 35th St, Milwaukee, in the State and Eastern District of Wisconsin, described in Attachment A, and seize the items described in Attachment B.

65. Based on the above information, I submit there is probable cause to believe that Omar Guevara, **Oscar Guevara**, **Maria Del Carmen Andrade**, and **Reynaldo Moguel-Bonilla** have committed violations of 18 U.S.C. Sections 1028 and 1546.

ATTACHMENT A

LOCATION TO BE SEARCHED

The multi-level single family residence located at 1610 South 35th St, Milwaukee, WI pictured below that also includes a small fenced back yard and white sided two-car garage that faces the alleyway:



ATTACHMENT B

Property to be Seized

1. Information or correspondence pertaining to violations of Title 18, United States Code, Sections 1028(a) and 1546, in any form wherever it may be stored or found, including but not limited to the following:

- a. Permanent resident cards, social security cards, and any other personal identification documents;
- b. Document or money ledgers, customer lists, correspondence, notations, logs, receipts, journals, books, records and other documents noting the quantity of documents produced, transferred or possessed and identifying document-making implements obtained or used for the purpose of producing or transferring fraudulent documents.
- c. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes documents and other items or lists reflecting names, addresses, telephone numbers and communications regarding illegal activities among and between members and associates involved in the fraudulent document activities;
- d. Photographic equipment, video equipment, related media and photographs suitable for use with permanent resident alien cards and other such personal identification documents;
- e. Storage media, computers, computer hardware, memory storage devices, flash drives, scanners, printers, floppy diskettes, computer software (herein referred to "computer"), computer related documentation,

manuals, passwords, printouts, peripherals, and other such materials that may contain evidence of the above violations, including ;

- i. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- ii. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;
- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;
- v. evidence of the times the computer was used;
- vi. passwords, encryption keys, and other access devices that may be necessary to access the computer;
- vii. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;
- viii. records of or information about Internet Protocol addresses used by the computer;

- ix. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - x. contextual information necessary to understand the evidence described in this attachment.
- f. Cellular telephones, SmartPhones, pagers, text messaging systems and other communication devices, including devices capable of sending, receiving, or storing e-mails, and any and all records associated with such communication services.
- g. Typewriters, cutting boards, templates, designs, images, card stock, laminating equipment, optical memory stripes, embossing devices, presses, stamps, seals, holograms, logos, samples, reference materials, and related materials.
- h. United States currency and other financial instruments traceable to the production, storage, or distribution of personal identification documents.
- i. Documents establishing residency of the premises.
- j. Any and all documents referenced above, whether stored digitally or on paper.
2. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as

writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

3. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
4. The term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.